UNIVERSIDAD DE GRANADA

Departamento de Álgebra
Facultad de Ciencia.

Relación De Ejercicios del Tema I

(*Conjuntos. Aritmética Entera y Modular. Anillos de polinomios y cuerpos finitos*)

Parte I. Elementos de Teoría de conjuntos y estructuras algebraicas básicas

Ejercicio I.1. *¿Cuáles de los siguientes conjuntos son conjuntos no vacíos?*

$a)$ $\{x \in \mathbb{N} |\, 2x+7=0\}$ $b)$ $\{x \in \mathbb{Z} |\, 3x+5=9\}$
$c)$ $\{x \in \mathbb{Q} |\, x^2+4=6\}$ $d)$ $\{x \in \mathbb{R} |\, x^2+4=6\}$
$e)$ $\{x \in \mathbb{R} |\, x^2+3x+3=0\}$ $f)$ $\{x \in \mathbb{C} |\, x^2+3x+3=0\}$.

Ejercicio I.2. *Se consideran los siguientes conjuntos:*

$$A=\{x,y,z,t,e,f,g\},\ B=\{2,x,\sqrt{-5},9,e^{\frac{3}{2}\pi},f,e\},\ C=\{z,2,a,b,d\}.$$

Determine los siguientes conjuntos definidos por:

$$A\cup B\cup C,\ A\cap B\cap C,\ A\setminus B,\ A\setminus(B\cup C),\ (A\cap B)\cup C,\ C\cap(B\setminus A).$$

Nota: Para dos conjuntos cualquiera, el operador $X\setminus Y$ indica el subconjunto de X cuyos elements no pertenecen a Y, i.e., $X\setminus Y=\{x\in X|\, x\notin Y\}$.

Ejercicio I.3. *Dados tres subconjuntos A, B y C de $\mathcal{X}$. Demuestre que las siguientes proposiciones son equivalentes:*

(i) $(A\cap C)\cup(B\cap\overline{C})=\emptyset$ *(ii)* $A\cap C=\emptyset,\ B\cap\overline{C}=\emptyset$
(iii) $C\subset\overline{A},\ B\subset C$ *(iv)* $B\subset C\subset\overline{A}$.

¿Que condición deben cumplir A y B para que hay un conjunto C con una de las propiedades $(i)\Leftrightarrow(ii)\Leftrightarrow(iii)\Leftrightarrow(iv)$?
Nota: Para un subconjunto cualquiera $Y\subseteq X$, el operador $\overline{Y}$ indica el complementario de Y en X, i.e., $\overline{Y}=\{x\in X|\, x\notin Y\}$.

Ejercicio I.4. *La notación $\times$ se refiere al producto cartesiano entre conjuntos.*

a). Demostrar que si $A\cup B\subseteq A\cup C$ y $A\cap B\subseteq A\cap C$ entonces $B\subseteq C$.

b). Probar que $(A\cup B)\times Y=(A\times Y)\cup(B\times Y)$ y que $(A\cap B)\times Y=(A\times Y)\cap(B\times Y)$.

c). Comprueba que se cumple

$$(A\times X)\cap(B\times Y)\ =\ (A\cap B)\times(X\cap Y).$$

d). Dar un ejemplo de conjuntos X_1,X_2,Y_1,Y_2 verificando

$$(X_1\times Y_1)\cup(X_2\times Y_2)\neq(X_1\cup X_2)\times(Y_1\cup Y_2).$$

Ejercicio I.5. *Se define el operador* $A\Delta B := (A \cup B) \setminus (A \cap B)$. *Demuestre que se cumplen las siguientes propiedades:*

$$A\Delta B = (A \setminus B) \cup (B \setminus A) \qquad A\Delta\emptyset = A$$
$$A\Delta A = \emptyset \qquad A\Delta(B\Delta C) = (A\Delta B)\Delta C$$
$$A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C) \qquad \overline{A\Delta B} = (A \cap B) \cup (\overline{A} \cap \overline{B})$$
$$(A\Delta B) \setminus C = (A \cup C)\Delta(B \cup C) \qquad \Big(A\Delta C = B\Delta C\Big) \Leftrightarrow \Big(A = B\Big).$$

Ejercicio I.6. *Sea* X *un conjunto cualquiera y* $\mathscr{P}(X)$ *el conjunto de todas las partes de* X. *Es decir, un elemento de* $\mathscr{P}(X)$ *ha de ser un subconjunto cualquiera de* X. [a)]

a). Calcule $\mathscr{P}(\{a,b,c,d\})$ *y* $\mathscr{P}\Big(\mathscr{P}(\{a,b,c,d\})\Big)$*;*

b). Cuantos elementos tiene $\mathscr{P}(\{a,b,c,d\})$*?;*

c). Cuantos subconjuntos tiene $\{a,b,c,d\}$ *con* 2 *elementos y cuantos con tres elementos?;*

d). Cuantos subconjuntos de k *elementos tiene un conjunto* X *con* n *elementos.*
Indicación: Observe que $k \leq n$. *Usa la inducción sobre* n.

e). Comprueba que si $X \subseteq Y$, *entonces* $\mathscr{P}(X) \subseteq \mathscr{P}(Y)$.

Ejercicio I.7. *Sea* $f : X \to Y$ *una aplicación entre conjuntos. Demuestre que se verifican las siguientes equivalencias:*

a). f es una aplicación inyectiva si y sólo si existe alguna aplicación $g : Y \to X$ *tal que* $g \circ f = 1_X$.

b). f es una aplicación sobreyectiva si y sólo si existe alguna aplicación $g : Y \to X$ *tal que* $f \circ g = 1_Y$.

Nota: Se llama $1_Z : Z \to Z$ *la aplicación* identidad *definida por* $1_Z(z) = z$, $\forall z \in Z$.

Ejercicio I.8. *Dadas dos aplicaciones* $\varphi : X \to Y$ *y* $\psi : Y \to Z$. *Demostrar*

a). Si φ *y* ψ *son inyectivas entonces* $\psi \circ \varphi$ *es inyectiva.*

b). Si $\psi \circ \varphi$ *es inyectiva entonces* φ *es inyectiva.*

c). Si $\psi \circ \varphi$ *es inyectiva y* φ *es sobreyectiva entonces* ψ *es inyectiva.*

d). Si ψ *y* φ *son sobreyectivas entonces* $\psi \circ \varphi$ *es sobreyectiva.*

e). Si $\psi \circ \varphi$ *es sobreyectiva y* φ *es inyectiva entonces* ψ *es sobreyectiva.*

Ejercicio I.9. *Sea* $f : X \to Y$ *una aplicación entre conjuntos. Se definen las siguientes aplicaciones entre sus correspondientes conjuntos de potencia:*

$$\begin{aligned} f^* : \mathscr{P}(Y) &\longrightarrow \mathscr{P}(X) \\ B &\longmapsto f^*(B) = \{x \in X \,|\, f(x) \in B\}, \end{aligned}$$

$$\begin{aligned} f_* : \mathscr{P}(X) &\longrightarrow \mathscr{P}(Y) \\ A &\longmapsto f_*(A) = \{y \in Y \,|\, y = f(a),\ \textit{para algún } a \in A\} \end{aligned}$$

[a)] Inclusive, por supuesto, el conjunto vacío, ya que este es un subconjunto de cualquier conjunto.

1. *Compruebe que f^* y f_* son bien definidas. ¿Es f^* inversa de f_*? En caso que no, de explícitamente un contra-ejemplo.*

2. *Demuestre que f es biyectiva, si y sólo si, f^* y f_* son mutuamente inversas* [b)].

3. *Demuéstrese que las siguientes condiciones son equivalencias:*

   3a). f es una aplicación inyectiva;

   3b). $f^*(f_*(A)) = A$, para cualquier elemento $A \in \mathscr{P}(X)$;

   3c). f^* es una aplicación sobreyectiva;

   3d). f_* es una aplicación inyectiva.

4. *Demuéstrese que las siguientes condiciones son equivalencias:*

   a). f es una aplicación sobreyectiva;

   b). $f_*(f^*(B)) = B$, para cualquier elemento $B \in \mathscr{P}(Y)$;

   c). f^* es una aplicación inyectiva;

   d). f_* es una aplicación sobreyectiva.

5. *Demostrar que, para cualquier $A \in \mathscr{P}(X)$ y $B \in \mathscr{P}(Y)$ se tiene que*

$$f_*\big(A \cap f^*(B)\big) \,=\, f_*(A) \cap B, \quad f^*\big(f_*(A) \cup B\big) \,=\, A \cup f^*(B).$$

Ejercicio I.10. *Dada la aplicación $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ definida por $f(t) = (t + 3, 2 - 3t)$, para cualquier $t \in \mathbb{R}$. Siguiendo la notación del* Ejercicio I.9, calcule: $f(5)$, $f_*([0, 1])$, $f_*([0, +\infty[)$, $f_*(\mathbb{R})$, $f^*(\{(0, 1)\})$, $f^*(\mathbb{R} \times \mathbb{R})$.

Ejercicio I.11. *Se denota por $|X|$ el cardinal del conjunto X* [c)]*. Sean A y B dos conjuntos con cardinal finito.*

a). Demostrar que:

$$\left|\left\{f : A \to B |\, f \text{ es una aplicación } \right\}\right| = |B|^{|A|}.$$

b). Probar que si $|A| \leq |B|$ entonces existe una inyección de A hacia B. Demostrar que

$$\left|\left\{f : A \to B |\, f \text{ es una aplicación inyectiva } \right\}\right| = |B|(|B| - 1) \cdots (|B| - |A| + 1).$$

Ejercicio I.12. *Se considera la siguiente función:*

$$f : \mathbb{R}^+ \setminus \{0\} \longrightarrow \mathbb{R},\ x \longmapsto f(x) = \frac{x}{1 + x}$$

a). Comprueba que f es inyectiva.

b). Hallar la expresión de $f^{(n)}(x) = \overbrace{f \circ f \circ \cdots \circ f}^{n\text{-veces}}(x)$. Calcular $f^{(n)}\left(\mathbb{R}^+ \setminus \{0\}\right)$.

Ejercicio I.13. *Determinar cuales de las siguientes aplicaciones son inyectivas, sobreyectivas o biyectivas:*

[b)] Es decir, que f^* en la inversa de f_* y vice-versa.

[c)] Para este curso se conviene de que *cardinal* de un conjunto significa el "número" de sus elementos.

a). $f : \mathbb{N} \to \mathbb{N},\ n \mapsto f(n) = n^2$;

b). $f : \mathbb{Q} \to \mathbb{R},\ x \mapsto f(x) = x^{-1}$;

c). $f : \mathbb{Z} \to \mathbb{Z},\ n \mapsto f(n) = n^2 + 1$;

d). $f : \mathbb{R} \to \mathbb{R},\ x \mapsto f(x) = |x|$.

Ejercicio I.14. *Sea* $D \subseteq \mathbb{R} \times \mathbb{R}$ *uno de los siguientes conjuntos*

$$\left\{(x,y)|x = y^2\right\},\ \left\{(x,y)|x^2 + y^2 = 1\right\},\ \left\{(x,y)|cos(x) = y\right\},\ \left\{(x,y)|y = e^x\right\}.$$

Calcular las imágenes de D *mediante la primera y la segunda proyección canónica* $\pi_i : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $i = 1, 2$.

Ejercicio I.15. *Definimos sobre el cuerpo* $\mathbb{R}$ *de los números reales la siguiente relación:*

$$x \mathscr{R} y \Leftrightarrow x - y \in \mathbb{Z}.$$

a). Probar que $\mathscr{R}$ *es una relación de equivalencia.*

b). Describir el conjunto cociente $\mathbb{R}/\mathbb{Z}$.

Responder a las mismas preguntas para la relación $x \mathscr{R} y \Leftrightarrow x - y \in 2\pi\mathbb{Z}$.

Ejercicio I.16. *En el conjunto* $\mathbb{Q}$ *de los números racionales se define la siguiente relación binaria:*

$$x \mathscr{R} y \Leftrightarrow \exists h \in \mathbb{Z},\ tal\ que\ x = \frac{3y + h}{3}.$$

a). Probar que $\mathscr{R}$ *es una relación de equivalencia.*

b). ¿Están $\frac{2}{3}$ *y* $\frac{4}{5}$ *en la misma clase?*

c). Describir el conjunto cociente $\mathbb{Q}/\mathscr{R}$.

Ejercicio I.17. *Sea el conjunto* $X = \{1, 2, 3\}$. *En el conjunto* $\mathscr{P}(X)$ *definimos la siguiente relación binaria:* $a \mathscr{R} b$ *si y sólo si la suma de todos los elementos de* a *es igual a la suma de los de* b.

a). Probar que $\mathscr{R}$ *es una relación de equivalencia.*

b). Describir el conjunto cociente $\mathscr{P}(X)/\mathscr{R}$.

Ejercicio I.18. *En el espacio* $\mathbb{R}^3$ *se considera la siguiente relación binaria:*

$$(x_1, x_2, x_3) \mathscr{R} (y_1, y_2, y_3) \Leftrightarrow x_3 = y_3.$$

a). Probar que $\mathscr{R}$ *es una relación de equivalencia.*

b). Describir geométricamente las clases de equivalencia.

Responder a la mismas preguntas para la relación

$$(x_1, x_2, x_3) \mathscr{R} (y_1, y_2, y_3) \Leftrightarrow \exists \lambda \in \mathbb{R}\ tal\ que\ x_i = \lambda y_i,\ i = 1, 2, 3.$$

Ejercicio I.19. *Considera en* $\mathbb{R}$ *la siguiente relación binaria:*

$$x \mathscr{R} y \Leftrightarrow x - y \in \mathbb{Q}.$$

a). ¿Es $\mathscr{R}$ *una relación de equivalencia?*

b). Calcula las clases de los elementos 0, $\frac{2}{3}$, π *y* $-\pi$.

Ejercicio I.20. *Considera en* $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ *la siguiente relación binaria:*

$$(x_1, x_2)\, \mathscr{R}\, (y_1, y_2) \Leftrightarrow x_1 y_1 = x_2 y_2.$$

a). ¿Es $\mathscr{R}$ *una relación de equivalencia?*

b). Calcula las clases de los elementos $(8, 4)$, $(0, 4)$, $(-7, 1)$ *y* $(3, -5)$.

Ejercicio I.21. *Se define en* $\mathbb{Z}$ *la siguiente relación binaria:*

$$x\, \mathscr{R}\, y \Leftrightarrow x - y \text{ es múltiplo de } 3.$$

a). ¿Es $\mathscr{R}$ *una relación de equivalencia?*

b). Prueba que si x *e* y *son pares, entonces* $[x] \neq [y]$.

c). ¿Que significa $[x] \cap [y] = \emptyset$, *y que significa* $[x] \cup [y] = \mathbb{Z}$?

d). Describe $\mathbb{Z}/\mathscr{R}$.

Ejercicio I.22. *En el plano* $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ *se define la siguiente relación binaria:*

$$(x_1, x_2)\, \mathscr{R}\, (y_1, y_2) \Leftrightarrow \frac{x_1 + x_2}{x_1^2 + x_2^2 + 1/2} = \frac{y_1 + y_2}{y_1^2 + y_2^2 + 1/2}.$$

a). Comprobar que $\mathscr{R}$ *es una relación de equivalencia.*

b). Hallar la clase de $[(a, b)]$ *en función del parámetro* $k = (a + b)/a^2 + b^2 + 1/2$.

c). Describir geométricamente el conjunto cociente $\mathbb{R}^2/\mathscr{R}$.

Ejercicio I.23. *Fijamos un entero* $m \in \mathbb{Z}$ *y consideramos en el conjunto* $\mathbb{Z}$ *la siguiente relación binaria:*

$$x\, \mathscr{R}_m\, y \Leftrightarrow x - y \text{ es múltiplo de } m.$$

a). Comprobar que $\mathscr{R}$ *es una relación de equivalencia.*

b). Para cada $x \in \mathbb{Z}$ *se denota por* $[x]$ *su clase de equivalencia. Comprueba que* $[x] = \{x + km | \, k \in \mathbb{Z}\}$.

c). Cuantos elementos tiene el conjunto cociente $\mathbb{Z}/\mathscr{R}_m$ *(que se denota por* $\mathbb{Z}_m := \mathbb{Z}/\mathscr{R}_m$*). Si* $m = 0$ *cuantas clases de equivalencia hay.*

d). Definimos sobre $\mathbb{Z}_m$ *las siguientes operaciones binarias:*$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ *enviando* $([x], [y]) \mapsto [x + y]$, $\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ *enviando* $([x], [y]) \mapsto [xy]$.

d).1. Demostrar que $(\mathbb{Z}_m, +)$ *es un grupo abeliano.*

d).2. Calcula las tablas de multiplicación y suma para $\mathbb{Z}_4$.

d).3. Comprueba que $(\mathbb{Z}_7 \setminus \{[0]\}, \cdot)$ *tiene estructura de grupo abeliano.*

d).4. Probar que $H = \{[0], [2], [4]\}$ *es un subgrupo de* $(\mathbb{Z}_6, +)$.

Ejercicio I.24. *Sea* X *un conjunto finito con* n *elementos (por ejemplo* $X = \{1, 2, 3, \cdots, n\}$*). Se define el conjunto* $\mathcal{S}_n$ *como el conjunto de todas las aplicación biyectiva de* X *hacia* X *(llamadas también* permutaciones*).*

a). Demostrar que $\mathcal{S}$ tiene una estructura de grupo con la operación viene dada por la composición.

b). Comprueba que $\mathcal{S}_n$ es finito y encuentra su cardinal. Calcule todos los elementos de $\mathcal{S}_3$.

c). Probar que para $n \geq 3$, $\mathcal{S}_n$ no es abeliano.

$\mathcal{S}_n$ se le llama el grupo simétrico *de n símbolos.*

Ejercicio I.25. *Sean $(G, \cdot)$ y $(L, *)$ dos grupos cualesquiera. Comprueba que el conjunto subyacente del producto cartesiano $G \times L$ admite una única estructura de grupo que convierta las proyecciones canónicas $pr_1 : G \times L \to G$ y $pr_2 : G \times L \to L$ en morfismos de grupos. Demostrar que para cualquier par de morfismos de grupos $f : R \to G$ y $g : R \to L$, donde $(R, \dagger)$ es otro grupo, existe un único morfismo de grupos $h : R \to G \times L$ tales que $pr_1 \circ h = f$ y $pr_2 \circ h = g$.*

Ejercicio I.26. *Sea $(G, \cdot)$ un grupo cualesquiera. Fijamos $g \in G$, se define la aplicación $\lambda_g : \mathbb{Z} \to G$ de tal manera que para cualquier $n \in \mathbb{Z}$ con $n > 0$ tenemos*

$$\lambda_g(n) = \underbrace{g \cdot g \cdot .... \cdot g}_{n\text{-veces}},\ \lambda_g(0) = e\,(\textit{elemento neutro}),\ \lambda_g(-n) = \underbrace{g^{-1} \cdot g^{-1} \cdot .... \cdot g^{-1}}_{n\text{-veces}}.$$

I.261 Demostrar que para cada $g \in G$, λ_g es un morfismo de grupos.

I.261 Probar que la imagen $\lambda_g(\mathbb{Z})$ es el subgrupo cíclico *de G generado por $g \in G$.*

Un grupo H se dice que es cíclico si existe un elemento $x \in H$ tal que para cualquier $a \in H$ se tiene $a = x^n$ para algún $n \in \mathbb{Z}$.

Ejercicio I.27. *Consideramos el plano real $\mathbb{C} := \mathbb{R} \times \mathbb{R}$. Dotaremos $\mathbb{C}$ de su estructura de grupo abeliano $(\mathbb{C}, +)$ definida como en el Ejercicio I.26, es decir $(a, b) + (c, d) = (a + b, c + d)$ cuyo elemento neutro es $\mathbf{0} = (0, 0)$. Ahora consideramos la siguiente operación interna: $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$, $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$, para cualquier $a, b, c, d \in \mathbb{R}$.*

a). Comprueba que la operación $\cdot$ es asociativa y conmutativa con elemento neutro $\mathbf{1} = (1, 0)$. Demostrar que $(\mathbb{C}^*, \cdot)$, donde $\mathbb{C}^* = \mathbb{C} \setminus \{\mathbf{0}\}$ es un grupo abeliano.

b). Probar que la aplicación $\iota : \mathbb{R} \to \mathbb{C}$ definida por $\iota(a) = (a, 0)$ es un morfismo inyectivo.

c). Sea $\mathsf{i} = (0, 1) \in \mathbb{C}$, comprobar que $\mathsf{i} \cdot \mathsf{i} = \mathsf{i}^2 = -\mathbf{1}$. Demostrar que cualquier elemento $z \in \mathbb{C}$ se expresa de forma única como $z = \iota(a) + \iota(b) \cdot \mathsf{i}$, para ciertos $a, b \in \mathbb{R}$.(Dado que ι es inyectiva podemos identificar los elementos de $\mathbb{R}$ con sus imágenes, así usaremos las expresiones del tipo $a + b\mathsf{i}$. El conjunto $\mathbb{C}$ admite la estructura de un cuerpo y contiene una copia del cuerpo $\mathbb{R}$ de los números reales, este es el cuerpo de los números complejos.*)*

d). Sea $\mathbb{S}$ el subconjunto del cuerpo de los números complejos $\mathbb{C}$ cuyos elementos son de forma $z = a + b\mathsf{i}$ tal que $a^2 + b^2 = 1$. Demostrar que $(\mathbb{S}, \cdot)$ es un grupo. ¿Que relación hay entre $\mathbb{S}$ y el grupo cociente $\mathbb{R}/2\pi\mathbb{Z}$?

Ejercicio I.28. *Sea $\omega = \frac{1}{\sqrt{2}}(1 + \mathsf{i}) \in \mathbb{C}$.*

a). Probar que $\omega^8 = 1$, pero $\omega^k \neq 1$, para todo $k = 1, 2, \cdots, 7$.

b). Demostrar que el conjunto $\{\omega^n | \, n \in \mathbb{N}, 1 \leq n \leq 7\}$ es un grupo abeliano con la multiplicación de $\mathbb{C}$.

Ejercicio I.29. *Consideramos el conjunto* $G = \{a+b\sqrt{3} | \, a, b \in \mathbb{Q}\}$ *como subconjunto del conjunto* $\mathbb{R}$ *de los números reales.*

a). Probar que $a + b\sqrt{3} = c + d\sqrt{3}$ *si y sólo si* $a = c$ *y* $b = d$.

b). Demostrar que G *es un grupo con la suma de* $\mathbb{R}$.

De otra parte consideramos el siguiente subconjunto del conjunto de las matrices cuadradas con entradas en $\mathbb{Q}$*:*

$$H = \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} | \, a, b \in \mathbb{Q} \right\}$$

c). Comprobar que H *es un grupo con la suma de matrices.*

d). Demostrar que existe un isomorfismo de grupos entre G *y* H.

Parte II. Aritméticas Entera y Modular.

Ejercicio II.1. *Usa los principios de inducción para probar las siguientes afirmaciones:*

1. $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N}$,
2. $1 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, $\forall n \in \mathbb{N}$,
3. $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$, $\forall n \in \mathbb{N} \setminus \{0\}$,
4. $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$, $\forall n \in \mathbb{N} \setminus \{0\}$,
5. $1 \times 3 + 2 \times 4 + 3 \times 5 + \cdots + n(n+1) = \frac{n(n+1)(2n+7)}{6}$, $\forall n \in \mathbb{N}$,
6. $\frac{1}{1\times 3} + \frac{1}{3\times 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$, $\forall n \in \mathbb{N}$,
7. $7^n - 1$ *es mltiplo de* 6, $\forall n \in \mathbb{N}$,
8. $7^{2n} + 16n - 1$ *es mltiplo de* 64, $\forall n \in \mathbb{N}$,
9. $a^{2n} - b^{2n}$ *es divisible por* $a + b$, $\forall n \in \mathbb{N}$,
10. $\frac{1}{2n} \leq \frac{1\times 3\times 5\times \cdots \times (2n-1)}{2\times 4\times 6\times \cdots \times (2n)}$, *para cualquier nmero natural* $n \geq 1$,
11. $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$, *para cualquier nmero natural* $n \geq 2$,
12. $2^n \geq 2n + 1$, *para cualquier número natural* $n \geq 3$,
13. $2^n \geq n^2$, *para cualquier número natural* $n \geq 4$,
14. *Si* $\{a_n\}_{n\in\mathbb{N}}$ *es una sucesión de números naturales que satisface*

$$\begin{aligned} a_0 = 1,\ a_1 = 2,\ a_2 = 3, \\ a_n = a_{n-1} + a_{n-2} + a_{n-3},\ \text{para } n \geq 3 \end{aligned}$$

entonces $a_n \leq 3^n$, *para cualquier número natural* $n \geq 1$.

15. Si $\{b_n\}_{n\in\mathbb{N}}$ *es una sucesión de números naturales que satisface*

$$\begin{aligned} b_0 \,=\, 3,\; b_1 \,=\, 7,\\ b_n \,=\, 3b_{n-1} - 2b_{n-2},\;\; \textit{para } n \geq 2 \end{aligned}$$

entonces $b_n \,\leq\, 2^{n+2} - 1$, *para cualquier número natural* $n \geq 0$.

Ejercicio II.2. *Encuentra una definición recursiva verificada por cada una de las siguientes secuencias de números enteros:*

(*a*) 8, 15, 22, 29, 36, 43, $\cdots$,
(*b*) 6, 12, 24, 48, 96, $\cdots$,
(*c*) 1, 3, 7, 15, 31, 63, $\cdots$.
(*d*) 1, 4, 9, 16, 25, 36, $\cdots$,
(*e*) 1, 9, 35, 91, 189, $\cdots$,

Ejercicio II.3. *Compruebe que, para todo* $n \in \mathbb{N}$

$$(2n+1)^2 \,+\, \Big(2n(n+1)\Big)^2 \;=\; \Big(2n(n+1)+1\Big)^2.$$

Complete las siguientes igualdades:

$$19^2 + 180^2 \,=\, (\centerdot)^2, \quad 313^2 - 312^2 \,=\, (\centerdot)^2.$$

Ejercicio II.4. *Para* $n \in \mathbb{N} \setminus \{0\}$, *sea* $\mathfrak{H}_n \,=\, 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, *el n-ésimo* ***número armónico***.

1. *Para todo* $n \in \mathbb{N}$, *demuestre que* $1 + \frac{n}{2} \leq \mathfrak{H}_{2^n}$.

2. *Demuestre que para cualquier* $n \in \mathbb{N} \setminus \{0\}$, *se tiene*

$$\sum_{j=1}^{n} j\mathfrak{H}_j \;=\; \left(\frac{n(n+1)}{2}\right)\mathfrak{H}_{n+1} \,-\, \left(\frac{n(n+1)}{4}\right).$$

3. *Para todo* $n \in \mathbb{N} \setminus \{0\}$, *demuestre que*

$$\sum_{i=0}^{n} \frac{1}{2i+1} \;=\; \mathfrak{H}_{2n+1} \,-\, \left(\frac{1}{2}\right)\mathfrak{H}_n.$$

Ejercicio II.5. *Encuentra los sistema de numeración, si existe alguno, para los que se verifica cada una de las siguientes igualdades:*

(1) $(3)_\bullet \times (4)_\bullet \;=\; (22)_\bullet$;
(2) $(25)_\bullet \times (13)_\bullet \;=\; (51)_\bullet$;
(3) $(41)_\bullet \times (14)_\bullet \;=\; (1224)_\bullet$;
(4) $(13)_\bullet{}^4 \;=\; (14641)_\bullet$;
(5) $(52)_\bullet \times (25)_\bullet \;=\; (1693)_\bullet$.

Notación: la simbología $(x)_\bullet$ *significa la expresión del número natural* x *en la base* $\bullet$.

Ejercicio II.6. *Calcula cada una de las siguientes sumas en su correspondiente sistema de numeración:*

(*i.*) $(323201)_4 + (21321)_4$
(*ii.*) $(45741)_9 + (18475)_9$
(*iii.*) $(44122)_5 + (2231)_5$
(*iv.*) $(24325)_6 + (11324)_6$
(*v.*) $(134561)_7 + (2135)_7$
(*vi*) $10 \times (1212)_3$

Ejercicio II.7. *De la expresión en base* 8 *de los naturales que en base* 2 *se escriben:*

(a) $(101101100010011010111)_2$ (c) $(10001000000100110)_2$
(b) $(1011101111011111)_2$

Ejercicio II.8. *Demuestra las siguientes afirmaciones:*

1. *Un número escrito en base* 10 *es par si y sólo si su última cifra es par;*
2. *Un número escrito en base* 10 *es mltiplo de* 3 *si y sólo si la suma de sus cifras es múltiplo de* 3*;*
3. *Un número escrito en base* 10 *es múltiplo de* 9 *si y sólo si la suma de sus cifras es múltiplo de* 9*;*
4. *Un número escrito en base* 10 *es mltiplo de* 5 *si acaba en* 0 *o en* 5*;*
5. *Un número escrito en base* 10 *es mltiplo de* 11 *si y sólo si la suma de sus cifras que ocupan un lugar* ***par*** *menos la suma de las cifras que ocupan posiciones* ***impares*** *es múltiplo de* 11*;*
6. *Un número escrito en base* 8 *es múltiplo de* 7 *si y sólo si la suma de sus cifras es múltiplo de* 7*.*

Ejercicio II.9. *Sea* b *un número natural.*

1. *Demuestra que si* $b \geq 3$*, entonces los números* $(b-1)^2$ *y* $2(b-1)$ *se escriben en base* b *como* $(xy)_b$ *y* $(yx)_b$ *respectivamente.*
2. *Si* $b \geq 1$*, representa* $2 \times (1 + 2 + 3 + \cdots + b)$ *en base* b*.*
3. *Si* $b \geq 4$*, comprueba que* $6 \times (1 + 2^2 + 3^2 + \cdots + b^2) = (2310)_b$*.*
4. *Aplica los apartados anteriores al valor* $b = 5$*.*

Ejercicio II.10. *Supongamos que* $4n+2$ *no es el cuadrado de ningún número entero. Comprueba que para* $n \geq 0$*, se tiene que*

$$E(\sqrt{n} + \sqrt{n+1}) = E(\sqrt{4n+2}).$$

NOTA*:* $E(a)$*, para un número real* a*, indica la parte entera del mismo.*

Ejercicio II.11. *Para cualquier número entero* $n > 0$*, comprueba que* $n! + 1$ *y* $(n+1)! + 1$ *son primos relativos (i.e., primos entre si).*

Ejercicio II.12. *Sea* $N \geq 3$ *un número entero primo a* 10 *(i.e.,* $\mathsf{mcd}(N, 10) = 1$*). Compruebe que* N *divide a un entero de la forma* $111\cdots1$ *(con* $k+1$ *cifras en la escritura décimal), es decir un entero de la form* $u_k = \sum_{j=0}^{k} 10^j$*.*
INDICACIÓN*: Aplica el algoritmo de división.*

Ejercicio II.13. *Para cualquier números enteros* a *y* b*, denotaremos por* $\mathsf{mcd}(a, b)$ *(respectivamente* $\mathsf{mcm}(a, b)$*) el máximo común divisor (respectivamente máximo común múltiplo) natural de* a *y de* b*. Comprueba las siguientes propiedades:*

1. *Si* $a|b$ *entonces* $\mathsf{mcd}(a, b) = |a|$*.*
2. $\mathsf{mcd}(a, \mathsf{mcd}(b, c)) = \mathsf{mcd}(\mathsf{mcd}(a, b), c) = \mathsf{mcd}(a, b, c)$ *(el máximo común divisor natural de* a, b, c*).*

3. $\mathsf{mcd}(ac, bc) = \mathsf{mcd}(a, b).c$.

4. *Si* $d|a$ *y* $d|b$ *entonces* $\mathsf{mcd}(\frac{a}{d}, \frac{b}{d}) = \frac{\mathsf{mcd}(a,b)}{d}$.

5. *Si* $a, b \in \mathbb{N}$ *entonces* $ab = \mathsf{mcd}(a, b).\mathsf{mcm}(a, b)$.

Ejercicio II.14. *Sean* a *y* b *dos números enteros. Demuestra que si* $\mathsf{mcd}(a, b) = 1$*, entonces*

- $\mathsf{mcd}(a + b, ab) = 1$,
- $\mathsf{mcd}(a - b, ab) = 1$.

Ejercicio II.15. *Sean* a *y* b *dos números enteros.*

1. *Si* $a = 105$ *y* $\mathsf{mcm}(a, b) = 1365$*. Cuales el valor de* b *sabiendo que* $\mathsf{mcd}(a, b) = 35$*?*

2. *Si* $a = 105$ *y* $\mathsf{mcm}(a, b) = 1365$*. Cuales el valor de* b *si* $\mathsf{mcd}(315, 3b) = 105$*?*

3. *Calcula* $\mathsf{mcd}(2520, 3675)$*,* $\mathsf{mcd}(666, 154)$*,* $\mathsf{mcd}(250, 111)$*,* $\mathsf{mcd}(660, 1176)$*. Encuentre los valores de los elementos* $u, v \in \mathbb{Z}$ *que verifican* $2520 \times u + 3675 \times v = \mathsf{mcd}(2520, 3675)$.

Ejercicio II.16. *Prueba que dado un número entero cualquiera* m *se verifica una de las siguientes posibilidades:* $m^2 \equiv 0[8]$*,* $m^2 \equiv 1[8]$*,* $m^2 \equiv 4[8]$*. Prueba que si* n *es un número entero e impar no divisible por* 3 *entonces* $n^2 \equiv 1[24]$.

Ejercicio II.17. *Resuelve las siguientes congruencias:*

(1.) $3x \equiv 2[5]$	(4.) $148x \equiv 38[665]$
(2.) $7x \equiv 4[10]$	(5.) $6x \equiv 3[4]$
(3.) $9x \equiv 3[12]$	(6.) $13x \equiv 71[380]$

Ejercicio II.18. *Resuelve, usando el Teorema Chino del resto, los siguientes sistemas de ecuaciones en congruencias:*

1.

$$\left\{\begin{array}{l} x \equiv 3\,[5] \\ 2x \equiv 1\,[7] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 2\,[3] \\ x \equiv 3\,[5] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 5\,[21] \\ 2x \equiv 4\,[8] \end{array}\right. \quad \left\{\begin{array}{l} 4x \equiv 1\,[7] \\ 5x \equiv 2\,[13] \end{array}\right. \quad \left\{\begin{array}{l} 7x \equiv 5\,[31] \\ x \equiv 4\,[6] \end{array}\right.$$

2.

$$\left\{\begin{array}{l} x \equiv 3\,[5] \\ x \equiv 4\,[7] \\ 2x \equiv 5\,[11] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 2\,[4] \\ 2x \equiv 3\,[11] \\ x \equiv 1\,[13] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 2\,[5] \\ 2x \equiv 3\,[7] \\ 2x \equiv 4\,[12] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 3\,[7] \\ x \equiv 1\,[4] \\ 2x \equiv 1\,[5] \end{array}\right. \quad \left\{\begin{array}{l} 3x \equiv 4\,[17] \\ x \equiv 3\,[4] \\ 2x \equiv 2\,[15] \end{array}\right.$$

3.

$$\left\{\begin{array}{l} x \equiv 2\,[3] \\ 2x \equiv 1\,[7] \\ x \equiv 2\,[11] \\ x \equiv 5\,[13] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 3\,[5] \\ 2x \equiv 1\,[3] \\ 4x \equiv 1\,[11] \\ 5x \equiv 2\,[17] \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 2\,[3] \\ x \equiv 1\,[4] \\ 3x \equiv 2\,[7] \\ 2x \equiv 1\,[11] \end{array}\right. \quad \left\{\begin{array}{l} 3x \equiv 2\,[13] \\ x \equiv 1\,[3] \\ 3x \equiv 2\,[5] \\ x \equiv 1\,[8] \end{array}\right. \quad \left\{\begin{array}{l} 4x \equiv 5\,[11] \\ 2x \equiv 1\,[3] \\ x \equiv 4\,[5] \\ 4x \equiv 3\,[21] \end{array}\right.$$

Ejercicio II.19. *Tres granjeros dividen en partes iguales el arroz que han cultivado en común y que este año no ha pasado de* 3 *toneladas. Fueron a mercados diferentes en los que se usaban medidas de peso diferentes: en un lugar era de* 7 *kilos, en otro de* 15 *kilos y en el ltimo de* 19 *kilos. Cada uno vendió todo lo que pudo en medidas enteras en sus respectivos mercados y a la vuelta al primer granjero le sobraban* 6 *kilos, al segundo* 11 *kilos y al tercero* 14 *kilos. Cuánto arroz habrán cultivado?*

Ejercicio II.20. *Un cocinero de un barco relató cómo había conseguido las dieciocho monedas de oro que llevaba:* Quince piratas atacaron un barco francés. Consiguieron un cofre lleno de monedas de oro. Las repartieron en partes iguales y me dieron las cinco que sobraban. Sin embargo, tras una tormenta murieron dos de ellos, por lo que los piratas juntaron todas sus monedas y las volvieron a repartir. A mí me dieron las diez que sobraban. Por último, tras una epidemia de peste murieron cinco de los piratas que an quedaban en pie, por lo que los supervivientes repitieron la misma operación. Sabiendo que en el cofre no caben más de dos mil quinientas monedas*, Cuántas monedas contenía el cofre?.*

Ejercicio II.21. *A lo largo de un proceso judicial, un juez decreta el pago de una indemnización millonaria y en partes iguales a diecinueve personas por parte de una compañía de seguros. Debido a un fallo judicial se descubre que una pareja no debió cobrar tal indemnización. Un segundo juez ordena la devolución del dinero y volver a efectuar el pago de nuevo. Después de que la compañía apelara el juicio, un tercer juez ordena la devolución del pago por parte de otras cinco personas y volver a repartir la indemnización de nuevo. Dos de ellos, no conformes con la sentencia, apelan al tribunal supremo, el cual obliga mediante una sentencia final a la compañía a pagar el doble de la indemnización a estos dos juntos con los que cobraron en el tercer juicio. La compañía de seguros tená pensado no pagar más de seismil millones. Así después de pagar la indemnización de la sentencia final, a la compañía le sobran* 3 *millones. Además, le sobran* 2 *millones del pago del primer juicio, del segundo* 1 *millón y del tercero* 5 *millones. Cuántos millones habrá pagado exactamente la compañía de seguros?*

Ejercicio II.22. *Estudia las soluciones en* $\mathbb{Z}$ *de las siguientes ecuaciones:*

(1.) $3x + 4y = 5$
(2.) $4x + 6y = 17$
(3.) $2625x + 120y = 45$
(4.) $14x + 21y = 45$
(5.) $360x + 1176y = 16$
(6.) $133x + 380y = 65$

Ejercicio II.23. *Demuestra que el conjunto de los números primos es infinito.*
INDICACIÓN*: Para cada número primo* p*, considera el subconjunto* $\mathcal{S}_{(p)} \subset \mathbb{Z}$ *de todos los múltiplos de* p *(i.e., el ideal generado por* p *en el anillo* $\mathbb{Z}$*). Denota por* $\mathcal{S}$ *la unión de todos los subconjunto* $\mathcal{S}_{(p)}$*, es decir* $\mathcal{S} = \bigcup_{p,\ primo} \mathcal{S}_{(p)}$*. Verifique ahora que el complementario de* $\mathcal{S}$ *en* $\mathbb{Z}$ *es el subconjunto* $\{1, -1\}$*.*

Ejercicio II.24. *Demuestra que si* p *es un número entero primo, entonces* $\sqrt{p}$ *es irracional. Comprueba si los siguientes números reales son irracionales o no:* $\sqrt{75}$*,* $\sqrt{17}$*,* $\sqrt{2017}$*.*

Ejercicio II.25. *Sea* $\varphi : \mathbb{N} \setminus \{0, 1\} \longrightarrow \mathbb{N}$ *la aplicación de Euler, a saber* $\varphi(m)$ *es el numero de elementos del conjunto* $\{0, 1, 2, \cdots, (m-1)\}$ *que son primos relativos con* m *(i.e., los elementos* $s \in \{0, 1, 2, \cdots, (m-1)\}$ *con* $\mathsf{mcd}(m, s) = 1$*).*

1. *Calcula* $\varphi(113400)$ *y* $\varphi(4225)$*.*
2. *Calcula el resto de dividir* 1573^{3881} *entre* 113400*.*
3. *Calcula el resto de dividir* 194481^{3361} *entre* 4225*.*

Ejercicio II.26. *Para cualquier número natural $m \geq 2$, denotaremos por $\mathscr{U}(\mathbb{Z}_m)$ el conjunto de unidades del anillo $\mathbb{Z}_m$. Comprueba que $\mathscr{U}(\mathbb{Z}_m)$ admite una estructura de grupo abeliano. Sean $m, n \in \mathbb{N} \setminus \{0, 1\}$ tal que $\mathsf{mcd}(m, n) = 1$. Demuestre que $\mathscr{U}(\mathbb{Z}_{mn}) \cong \mathscr{U}(\mathbb{Z}_n) \times \mathscr{U}(\mathbb{Z}_m)$ isomorfos como grupos abelianos De un isomorfismo?. Como aplicación calcule los elementos de $\mathscr{U}(\mathbb{Z}_{126})$.*

Ejercicio II.27. *Sean a, $b \in A$ dos elementos en un anillo conmutativo. Decimos que a y b tienen un máximo común divisor si existe un elemento $d \in A$ tal que $d|a$ y $d|b$ y para cualquier elemento $c \in A$ con $c|a$ y $c|b$, se tiene que $c|d$. Se denota por $\mathsf{MCD}(a, b)$ el conjunto de los elementos que son máximo común divisor de a y de b.*

a). Determina en $\mathbb{Z}_2$ el subconjunto $\mathsf{MCD}(2, 7)$.

b). Determina en $\mathbb{Z}_{14}$ el subconjunto $\mathsf{MCD}(10, 12)$.

c). Determina en $\mathbb{Z}_{20}$ el subconjunto $\mathsf{MCD}(14, 18)$.

Ejercicio II.28 (Variante del algoritmo de división)**.** *Dada una fracción rational $x \in \mathbb{Q}$, comprueba que existe un entero $q' \in \mathbb{Z}$ tales que $|x - q'| \leq \frac{1}{2}$. Aplica tal resultado para poder dar una demostración de la siguiente afirmación: Dados dos números enteros $n, d \in \mathbb{Z}$ con $d \neq 0$, existen dos enteros $q', r' \in \mathbb{Z}$ tales que*

$$n \;=\; q'd + r' \quad y \quad |r'| \leq \frac{1}{2}|d|$$

(Tenga en cuenta sin embargo que r' no es siempre únicamente definido con esas condiciones cuando d es par).

Ejercicio II.29. *Compruebe que la siguiente ecuación:*

$$5x^3 + 11x^3 + 13x^3 \;=\; 0$$

ne admite más soluciones en $\mathbb{Z}^3$ que la solución trivial $(0, 0, 0)$.

Ejercicio II.30. *Demuestre que hay un numero infinito de números primos de las siguientes formas:*

$$4n - 1, \qquad 6n - 1$$

para n natural ≥ 2.

Parte III. Anillos de polinomios en una variable y cuerpos finitos

Ejercicio III.1. *En el conjunto*

$$\mathbb{Z}[\sqrt{D}] \;=\; \{a + b\sqrt{D} |\; a, d \in \mathbb{Z}\},$$

siendo D un entero, se consideran las operaciones

$$(a_1 + b_1\sqrt{D}) + (a_2 + b_2\sqrt{D}) \;=\; (a_1 + a_2) + (b_1 + b_2)\sqrt{D}$$

y

$$\Big((a_1 + b_1\sqrt{D})\Big)\Big((a_2 + b_2\sqrt{D})\Big) \;=\; (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)\sqrt{D}$$

Probar que es un anillo conmutativo. Probar también que cuando D no es un cuadrado perfecto [d] este anillo es un dominio de integridad. Como aplicación demuestra que $\mathbb{Z}[\sqrt{2}]$ es un dominio de integridad [e] y que $(1 + \sqrt{2})$ es una unidad en $\mathbb{Z}[\sqrt{2}]$.

[d] Un número entero m, se dice que es un *cuadrado perfecto* si existe un número natural n tal que $m^2 = n$

[e] Es decir, no tiene divisores no nulos de cero.

Ejercicio III.2. *Demuestra que todo dominio de integridad con un número finito de elementos es un cuerpo.*

Ejercicio III.3. *Un elemento de un anillo se dice que es idempotente si $a^2 = a$. Demuestra que en un dominio de integridad los únicos idempotentes son el cero y el uno. Demuestra que si a es idempotente entonces $(1 - a)$ también lo es. Calcula los elementos idempotentes de $\mathbb{Z}_6$, $\mathbb{Z}_8$ y $\mathbb{Z}_{12}$.*

Ejercicio III.4. *Un anillo A se dice que tiene característica p si p es el menor número natural tal que $1 + \overset{p \text{ veces}}{\cdots} + 1 = 0$. Si no existe tal p se dice que A tiene característica 0. Calcula las características de $\mathbb{Z}$ y $\mathbb{Z}_n$. Si A es un dominio de integridad, demuestra que su característica es 0 o un úmero primo.*

Ejercicio III.5. *Calcula la suma y el producto de las siguientes parejas de polinomios considerados en los anillos $\mathbb{Z}[\mathsf{x}]$, $\mathbb{Z}_6[\mathsf{x}]$ y $\mathbb{Z}_7[\mathsf{x}]$.*

(1) $p(\mathsf{x}) = 3\mathsf{x}^2 + \mathsf{x} + 5$, $q(\mathsf{x}) = \mathsf{x}^3 - \mathsf{x} + 3$;

(2) $p(\mathsf{x}) = 3\mathsf{x}^2 - 2\mathsf{x} + 3$, $q(\mathsf{x}) = \mathsf{x}^3 + 2\mathsf{x} - 3$;

(3) $p(\mathsf{x}) = 3\mathsf{x}^2$, $q(\mathsf{x}) = 2\mathsf{x}$;

(4) $p(\mathsf{x}) = 2\mathsf{x}^3 + 3\mathsf{x}^2 + 1$, $q(\mathsf{x}) = \mathsf{x}^2 + 2\mathsf{x} + 3$;

(5) $p(\mathsf{x}) = 5\mathsf{x}^4 + 2\mathsf{x}^2 + 4$, $q(\mathsf{x}) = 3\mathsf{x}^3 + 4\mathsf{x} - 2$;

(6) $p(\mathsf{x}) = 5\mathsf{x}^3 - \mathsf{x}^2 + 2$, $q(\mathsf{x}) = \mathsf{x}^2 + 3$.

Ejercicio III.6. *Calcula el cociente y el resto de la división para las siguientes parejas de polinomios considerados en los anillos $\mathbb{R}[\mathsf{x}]$, $\mathbb{Q}[\mathsf{x}]$, $\mathbb{Z}_5[\mathsf{x}]$ y $\mathbb{Z}_7[\mathsf{x}]$.*

(1) $p(\mathsf{x}) = \mathsf{x}^4 - 2\mathsf{x} + 1$, $q(\mathsf{x}) = 2\mathsf{x}^2 + 1$;

(2) $p(\mathsf{x}) = \mathsf{x}^5 - \mathsf{x}^3 + 3\mathsf{x} - 5$, $q(\mathsf{x}) = \mathsf{x}^2 + 5$;

(3) $p(\mathsf{x}) = \mathsf{x}^8 + \mathsf{x}^4 + 1$, $q(\mathsf{x}) = \mathsf{x}^2 - \mathsf{x} + 1$;

(4) $p(\mathsf{x}) = \mathsf{x}^5 - \mathsf{x}^2 + 1$, $q(\mathsf{x}) = \mathsf{x}^2 + 2\mathsf{x} + 3$;

(5) $p(\mathsf{x}) = \mathsf{x}^5 - \mathsf{x}^3 + 3\mathsf{x} - 5$, $q(\mathsf{x}) = \mathsf{x}^2 + 7$;

(6) $p(\mathsf{x}) = 2\mathsf{x}^4 + 3\mathsf{x}^3 + \mathsf{x}^2 + 6\mathsf{x} + 1$, $q(\mathsf{x}) = 3\mathsf{x}^2 + 1$.

Ejercicio III.7. *Halla un máximo común divisor y un mínimo común múltiplo en $\mathbb{Q}[\mathsf{x}]$, $\mathbb{Z}_3[\mathsf{x}]$ y $\mathbb{Z}_5[\mathsf{x}]$ de las siguientes prejas*

(1) $p(\mathsf{x}) = \mathsf{x}^2 - 1$, $q(\mathsf{x}) = \mathsf{x}^3 - 3\mathsf{x}^2 + 6\mathsf{x} - 4$;

$q(\mathsf{x}) = \mathsf{x}^3 - 3\mathsf{x}^2 + 2\mathsf{x} - 1$;

(2) $p(\mathsf{x}) = \mathsf{x}^2 + 2\mathsf{x} + 1$, $q(\mathsf{x}) = \mathsf{x}^3 + 7\mathsf{x}^2 + 15\mathsf{x} + 9$;

(3) $p(\mathsf{x}) = \mathsf{x}^5 + 5\mathsf{x}^4 + 4\mathsf{x}^3 + 3\mathsf{x}^2 + 2\mathsf{x} - 1$,

(4) $p(\mathsf{x}) = \mathsf{x}^4 + 2\mathsf{x}^2 + 1$, $q(\mathsf{x}) = \mathsf{x}^4 - 1$;

(5) $p(\mathsf{x}) = \mathsf{x}^4 + 2\mathsf{x}^2 + 1$, $q(\mathsf{x}) = \mathsf{x}^2 + 2$.

Encuentra en cada caso polinomios $u(\mathsf{x})$ y $v(\mathsf{x})$ tales que

$$p(\mathsf{x})u(\mathsf{x}) + q(\mathsf{x})v(\mathsf{x}) = \mathsf{mcd}(p(\mathsf{x}), q(\mathsf{x}))$$

Ejercicio III.8. *Estudia en $\mathbb{Q}[\mathsf{x}]$ los siguientes sistemas*

1. $(\mathsf{x}^4 + 2\mathsf{x} + 1)u(\mathsf{x}) + (\mathsf{x}^4 - 1)v(\mathsf{x}) = 3\mathsf{x}^3 + 3\mathsf{x}$;
2. $(\mathsf{x}^3 - \mathsf{x}^2 + 2\mathsf{x} - 1)u(\mathsf{x}) + (\mathsf{x}^2 + 2\mathsf{x} - 3)v(\mathsf{x}) = \mathsf{x} - 1$.

Ejercicio III.9. *Resuelve en $\mathbb{Z}_7[\mathsf{x}]$ los siguientes sistemas de congruencias*

$$\begin{cases} (3\mathsf{x}^3 + 2\mathsf{x} + 1)p(\mathsf{x}) \equiv (2\mathsf{x}^2 + 2)\left[\mathsf{x} + 2\right] \\ (2\mathsf{x}^2 + 2\mathsf{x})p(\mathsf{x}) \equiv 3\left[\mathsf{x} + 4\right]; \end{cases}$$

$$\begin{cases} (\mathsf{x}^2 + 6)p(\mathsf{x}) \equiv (\mathsf{x}^2 - 5\mathsf{x} + 1)\left[\mathsf{x} - 1\right] \\ p(\mathsf{x}) \equiv (\mathsf{x}^4 - \mathsf{x}^3 + 2\mathsf{x}^2)\left[\mathsf{x}^2 - \mathsf{x} + 1\right]. \end{cases}$$

Ejercicio III.10.

- *Demuestra que el polinomio* $\mathsf{x}^n + 1$ *no tiene raíces múltiples es* $\mathbb{R}$.
- *Encuentra todas las raíces de* $\mathsf{x}^2 - 1$ *en* $\mathbb{Z}_8[\mathsf{x}]$.
- *Calcula las raíces en* $\mathbb{Z}_5$ *del polinomio* $\mathsf{x}^2 + \mathsf{x} + 4$.
- *Calcula las raíces en* $\mathbb{Z}_7$ *del polinomio* $\mathsf{x}^3 - 6\mathsf{x} - 5$.
- *Determina cuáles de los siguientes polinomios tiene raíces múltiples en* $\mathbb{C}$
  1. $\mathsf{x}^3 - 3\mathsf{x}^2 + 3\mathsf{x} - 1$;
  2. $\mathsf{x}^3 + \mathsf{x}^2 + 1$;
  3. $\mathsf{x}^4 + \mathsf{x}^3 + \mathsf{x}^2 + \mathsf{x} + 1$.

Ejercicio III.11 (Fórmula de interpolación de Lagrange)**.** *Si* $a_0, \cdots, a_n$ *son elementos diferentes de un cuerpo* $\mathbb{K}$*, se definen los polinomios*

$$q_i(\mathsf{x}) \;=\; \prod_{i \neq j} (\mathsf{x} - a_i), \quad i = 0, 1, \cdots, n.$$

Dados $n+1$ *valores* $b_0, b_1, \cdots, b_n$ *en* $\mathbb{K}$ *prueba que el polinomio iterpolador de Lagrange*

$$p(\mathsf{x}) \;=\; \sum_{i=0}^{n} b_i c_i^{-1} q_i(\mathsf{x})$$

con $c_i = q_i(a_i)$*, es el único polinomio de grado menor o igual a* n *tal que* $p(a_i) = b_i$.

- *Calcula un polinomio* $L(\mathsf{x})$ *en* $\mathbb{Q}[\mathsf{x}]$ *tal que* $L(2) = 0$, $L(1) = -2$, $L(3) = 1$ *y* $L(-1) = 2$.
- *Calcula un polinomio* $L(\mathsf{x})$ *en* $\mathbb{Z}_5[\mathsf{x}]$ *tal que* $L(2) = 1$, $L(3) = 2$ *y* $L(4) = 1$.

Ejercicio III.12. *Estudia la irreducibilidad en* $\mathbb{Q}[\mathsf{x}]$ *de los siguientes polinomios:*

(1) $\mathsf{x}^4 + 3\mathsf{x}^3 + 4\mathsf{x}^2 + 6\mathsf{x} + 4$;

(2) $\mathsf{x}^5 + 6\mathsf{x}^2 - 12$;

(3) $\mathsf{x}^3 + 6\mathsf{x}^2 + 5\mathsf{x} + 25$;

(4) $2\mathsf{x}^4 - 8\mathsf{x}^2 + 8\mathsf{x} + 1$;

(5) $\mathsf{x}^4 - 2\mathsf{x}^2 - \mathsf{x} + 2$;

(6) $\mathsf{x}^3 + \mathsf{x} + 1$;

(7) $\mathsf{x}^4 + 6\mathsf{x}^3 + 5\mathsf{x}^2 + 14$;

(8) $\mathsf{x}^4 - 5\mathsf{x}^2 - 25$.

Ejercicio III.13. *Estudia la irreducibilidad de* $\mathsf{x}^2 + 1$ *y* $\mathsf{x}^3 + \mathsf{x} + 2$ *en* $\mathbb{Z}_3[\mathsf{x}]$ *y en* $\mathbb{Z}_5[\mathsf{x}]$*. Demuestra que el polinomio* $\mathsf{x}^4 + \mathsf{x} + 1$ *es irreducible en* $\mathbb{Z}_2[\mathsf{x}]$ *y que los polinomios* $\mathsf{x}^2 + 1$, $\mathsf{x}^3 + \mathsf{x} + 1$, $\mathsf{x}^4 + 2$ *son irreducibles en* $\mathbb{Z}[\mathsf{x}]$.

Ejercicio III.14. *Demuestra que si* p *es un número primo y* $\mathfrak{m}(\mathsf{x})$ *es un polinomio irreducible en* $\mathbb{Z}_p[\mathsf{x}]$*, entonces el conjunto cociente* $\mathbb{Z}_p[\mathsf{x}]_{\mathfrak{m}(\mathsf{x})}$ *tiene* $p^{\text{grado}(\mathfrak{m}(\mathsf{x}))}$ *elementos. Cuántos elementos tiene el anillo* $\mathbb{Z}_5[\mathsf{x}]_{\mathsf{x}^2+2\mathsf{x}+1}$*? Demustra que el polinomio* $\mathsf{x}^4 + \mathsf{x}^2 + \mathsf{x} + 1$ *es irreducible en* $\mathbb{Z}_3[\mathsf{x}]$*. Cuántas unidades tiene el anillo cociente* $\mathbb{Z}_3[\mathsf{x}]_{\mathsf{x}^4+\mathsf{x}^2+\mathsf{x}+1}$*? Calcula la imagen del polinomio* $\mathsf{x}^5 + \mathsf{x}^2 + \mathsf{x} \in \mathbb{Z}_3[\mathsf{x}]$ *en el anillo cociente* $\mathbb{Z}_3[\mathsf{x}]_{\mathsf{x}^4+\mathsf{x}^2+\mathsf{x}+1}$.

Ejercicio III.15.

1. *Demuestre que* $\mathsf{x}^2+\mathsf{x}+1$ *es un polinomio irreducible en* $\mathbb{Z}_5[\mathsf{x}]$.

2. *Sea* $P \in \mathbb{Z}_5[\mathsf{x}]$ *un polinomio irreducible de grado dos con coeficiente líder* 1. *Demuestre que el cuerpo cociente* $\mathbb{Z}_5[\mathsf{x}]/\langle P\rangle$ *es isomorfo a un cuerpo finito de* 25 *elementos, digamos* $\mathbb{F}_{25}$. *Compruebe que* P *tiene dos raíces en* $\mathbb{F}_{25}$

3. *Denotemos por* α *una raíz de* $\mathsf{x}^2+\mathsf{x}+1$ *en* $\mathbb{F}_{25}$. *Demuestre que, cualquier* $\beta \in \mathbb{F}_{25}$ *es de forma* $\beta = a\alpha + b$, *para algún para de elementos* $a, b \in \mathbb{Z}_5$

4. *Sea* $T(\mathsf{x}) = \mathsf{x}^5 - \mathsf{x} + 1$. *Demuestre que para cualquier* $\beta \in \mathbb{F}_{25}$, *se tiene que* $T(\beta) \neq 0$. *Deducir pues que* T *es irreducible sobre* $\mathbb{Z}_5$. *¿Podemos concluir que* T *es irreducible sobre* $\mathbb{Q}$*?*

Ejercicio III.16. *Sea* $P(\mathsf{x}) = \mathsf{x}^4 - 10\mathsf{x}^3 + 21\mathsf{x}^2 - 10\mathsf{x} + 11$ *un polinomio de* $\mathbb{Z}[\mathsf{x}]$.

1. *Descompone* P *en factores irreducibles módulo:* $2, 3$ *y* 5.

2. *Demuestre que* P *es un polinomio irreducible sobre* $\mathbb{Q}$.

Ejercicio III.17. *Denotemos por* $\mathbb{K}$ *el anillo cociente* $\mathbb{Z}_3[\mathsf{x}]/\langle \mathsf{x}^3 + 2\mathsf{x} + 1\rangle$.

1. *Demostrar que* $\mathbb{K}$ *es un cuerpo con* 27 *elementos.*

2. *Compruebe que la clase de equivalencia* $\overline{\mathsf{x}}$ *de* x *en* $\mathbb{K}$, *es un generador del grupo* $\mathbb{K}^\times$ [f)].

3. *Encuentre el número natural* n *tales que* $\overline{\mathsf{x}}^2 + \overline{\mathsf{x}} = \overline{\mathsf{x}}^n$.

Ejercicio III.18. *Sea* $\mathbb{K}$ *un cuerpo finito con* q *elementos y de característica* p *impar.*

1. *Compruebe que la aplicación*
$$\begin{aligned} \varphi : \mathbb{K}^\times &\longrightarrow \mathbb{K}^\times \\ x &\longmapsto x^2 \end{aligned}$$
es un morfismo de grupos donde el subgrupo imagen $\mathrm{Im}(\varphi)$ *tiene indice* 2 *en* $\mathbb{K}^\times$ [g)].

2. *Sea* $x \in \mathbb{K}^\times$; *demuestre que* x *es un cuadrado en* $\mathbb{K}$ *si y solamente si,* $x^{\frac{q-1}{2}} = 1$.

3. *Demuestre que* -1 *es un cuadrado en* $\mathbb{K}$ *si y solamente si,* $q \equiv 1[4]$.

4. *a) Sea* $\mathbb{L}$ *un cuerpo que contenga a* $\mathbb{K}$ *sobre el cual el polinomio* X^4+1 *admite una raíz* α. *Verifique que se cumple:*
$$\left(\alpha + \alpha^{-1}\right)^2 = 2$$
b) Deduce que 2 *es un cuadrado en* $\mathbb{K}$ *si y solamente si,* $q \equiv (\pm 1)[8]$.

Ejercicio III.19. *Consideramos* $\mathbb{Z}_p$ *el cuerpo cociente de* $\mathbb{Z}$ *módulo un primo* p.

1. *Factoriza* $X^4 + 1$ *en* $\mathbb{Z}_p$. *Para ello distingue entre los casos:* $p = 2$, $p \equiv 1[8]$, $p \equiv -3[8]$, $p \equiv -1[8]$ *ó* $p \equiv 3[8]$; *luego usa el Ejercicio III.18.*

2. *Demuestre que* $X^4 + 1$ *es un polinomio irreducible en* $\mathbb{Q}$.

Ejercicio III.20. *Sea* p *un número primo y* $\mathbb{K}$ *un cuerpo finito de característica distinta de* p.

[f)] Eso es que cualquier elemento del grupo es una potencia de $\overline{\mathsf{x}}$.

[g)] El indice de un subgrupo: Sea G un grupo abelian y H un subgrupo de G. Se define el *índice* de H como el cardinal del conjunto cociente G/H definido a su vez mediante la relación de equivalencia: $x \sim y \Leftrightarrow \exists\, h \in H$ tq $y = hx$.

1. *Sea P un factor irreducible en $\mathbb{K}[X]$ del polinomio*

$$\Phi_p(X) \;=\; X^{p-1} + X^{p-2} + \cdots + X + 1$$

Consideramos el cuerpo cociente $\mathbb{L} = \mathbb{K}[X]/\langle P\rangle$ y $\alpha = \overline{X} \in \mathbb{L}$ la clase de equivalencia de X módulo P. Demuestre que α, como elemento de $\mathbb{L}^\times$, es de orden p [h)] y deducir que

$$|\mathbb{K}|^d \;\equiv\; 1[p],$$

donde d es el grado de P y $|\mathbb{K}|$ es el cardinal de $\mathbb{K}$.

2. *Supongamos que la clase de equivalencia $\overline{|\mathbb{K}|}$ engendra (o es un generador del) el grupo multiplicativo ${\mathbb{Z}_p}^\times$. Demuestre que Φ_p es irreducible en $\mathbb{K}[X]$.*

3. *Deduce que si q es primo tale que $\overline{q}$ engendra a $\mathbb{Z}_p^\times$, entonces Φ_p es irreducible en $\mathbb{Z}_q[X]$.*

4. *Sean p, q dos números primos. Supongamos que $q \neq 2$, $p \equiv -1[3]$ y que $\overline{q}$ engendra $\mathbb{Z}_p^\times$. Demuestre que*

$$X^{p+1} - X + q \in \mathbb{Q}[X]$$

es un polinomio irreducible (Ind. reduce módulo q y módulo 2, luego usa el pregunta anterior).
***Aplicación**: Demuestre que el polinomio $X^{18} - X + 3$ es irreducible sobre $\mathbb{Q}$.*

[h)] Eso es que p es el más pequeño entre los números naturales n que satisfacen $\alpha^n = 1$.